www.cyhawk-africa.com

JUNE 2025

REPORT OF THE CYBER THREAT LANDSCAPE IN AFRICA

By
Hassanat Oladeji

Executive Summary

In June 2025, the cyber threat landscape across Africa was dominated by extensive attacks on government infrastructure, primarily through database breaches and unauthorized access. Morocco and Algeria emerged as the most targeted countries, accounting for the majority of incidents tracked this month.

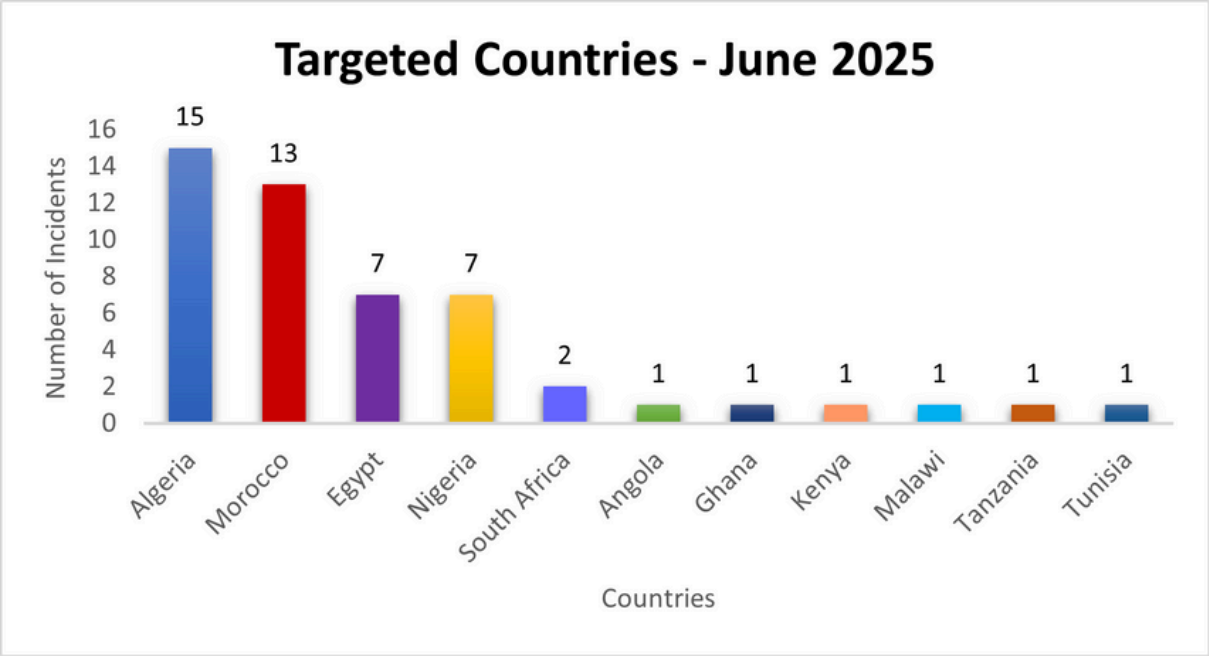
A small cluster of threat actors drove most of this activity, leveraging database compromises and credential-based intrusions. Industries outside of government, such as financial services, education, insurance, healthcare, aviation, and sport, were also affected, underscoring the widening scope of threat actor campaigns.

This report highlights critical gaps in cybersecurity, especially in public infrastructure, and calls for urgent action to strengthen defenses across the region.

The analysis is based on a dataset of 50 cybersecurity incidents recorded between 1 June and 30 June 2025. The dataset includes the following fields:

- *S/No: Incident identifier*
- *Date: Date of the incident*
- *Threat Actor: Group or individual responsible*
- *Country: Targeted country*
- *Threat Type: Nature of the attack (e.g., database breach, defacement, ransomware)*
- *Industry: Sector targeted (e.g., government, education, telecommunications)*

TARGETED COUNTRIES IN AFRICA



Morocco and Algeria accounted for more than half of all incidents combined, making them the epicenter of cyber activity during this period.

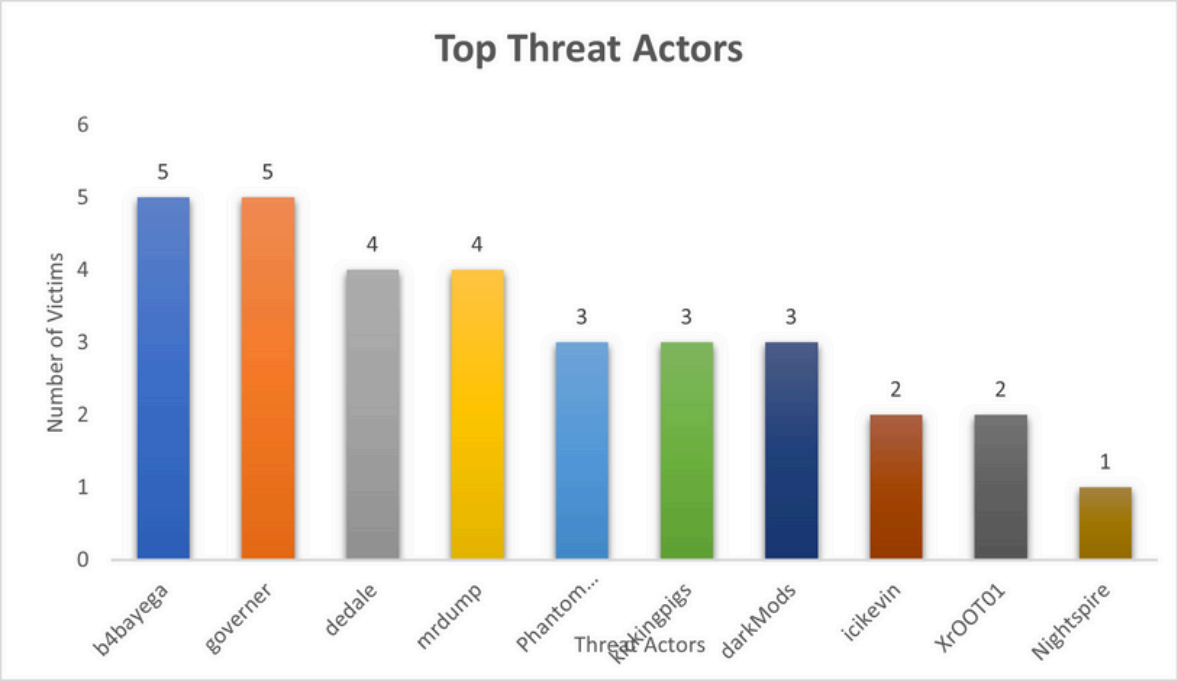
Algeria had 15 incidents, while Morocco had 13 incidents.

Other highly targeted countries include:

- Egypt – 7 incidents
- Nigeria– 7 incidents
- South Africa – 2 incidents

Additional countries like Angola, Ghana, Kenya, Malawi, Tanzania, and Tunisia were each hit once, signaling a broader regional threat distribution across Africa.

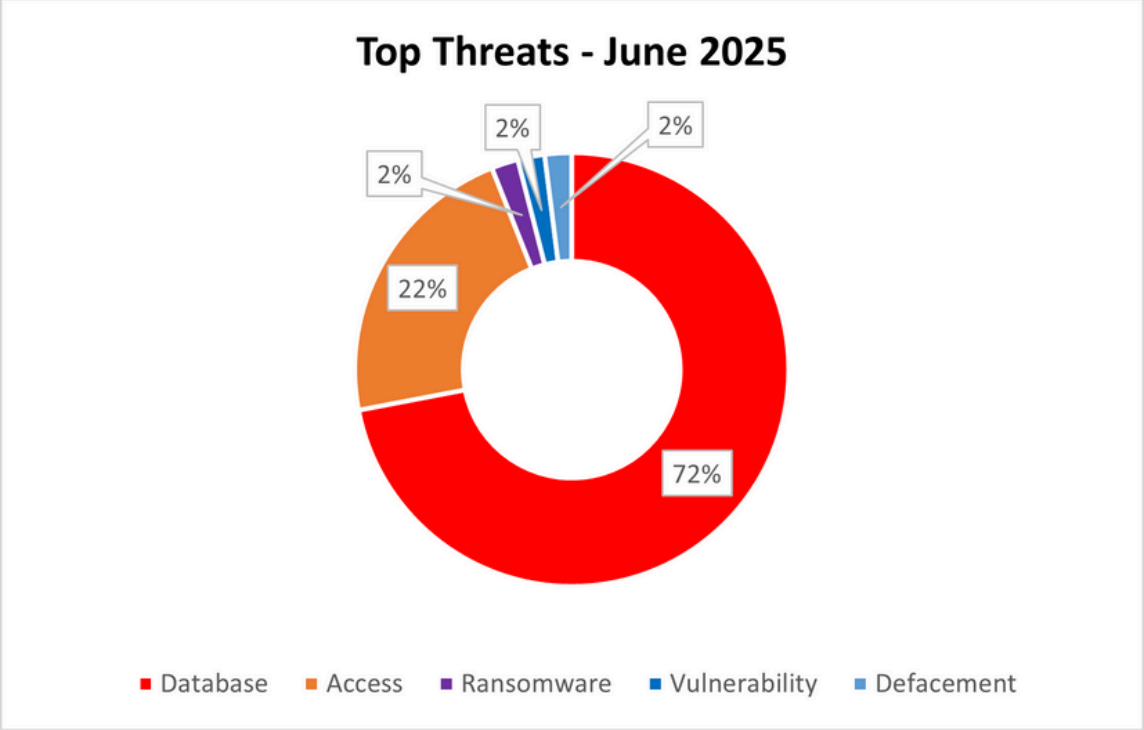
MOST ACTIVE THREAT ACTORS



Our analysis revealed that a relatively small circle of highly active threat actors, b4bayega and governer, was responsible for most of the incidents across Africa, with a major concentration in Morocco and Algeria. These actors employed a mix of tactics, including database breaches and compromised access attacks, often targeting critical government systems but also probing other industries such as financial services, education, aviation, healthcare, insurance, and sports.

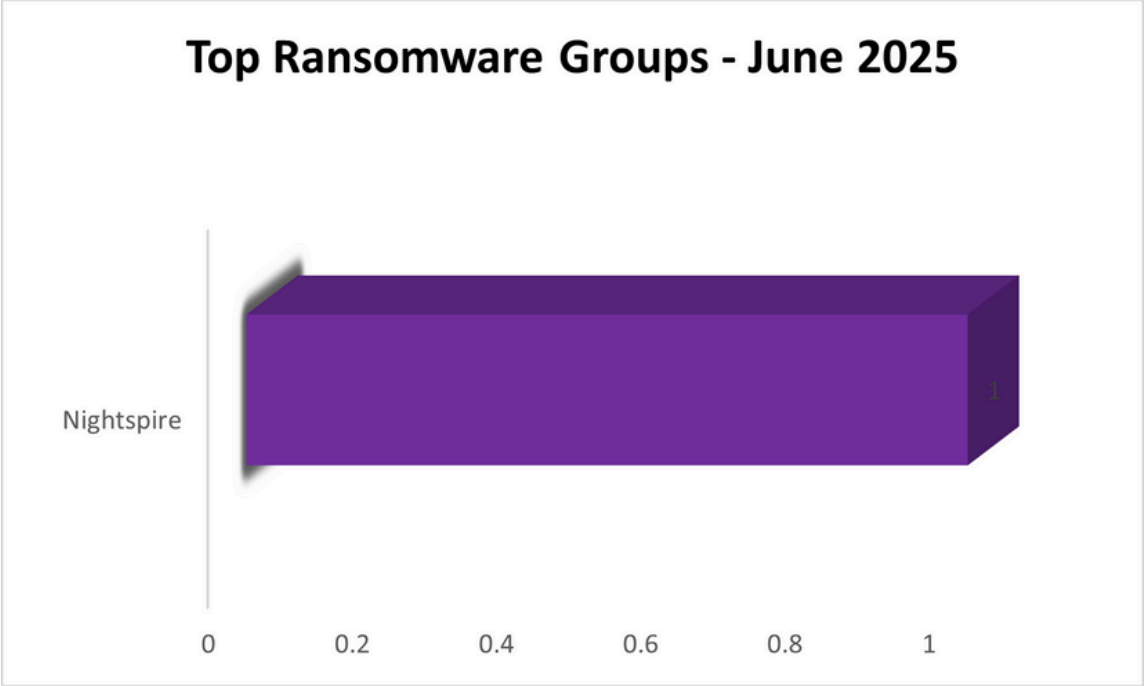
- kill9_x was involved in 6 attacks, mainly related to database leaks of 5 financial and 1 government institutions.
- Phantom Atlas (3 incidents) targeted only Algeria across the financial services and telecommunications industry.
- B4baYega (3 incidents) and Nightspire (2 incidents) showed limited but specific targeting behavior.
- Other actors like Libyantest, El_farado, Datacarry, Everest, and Team1722 were linked to 1 incident each, indicating either isolated operations or early activity phases.

TOP THREATS



- Database Breaches were the most common threat, making up about 72% of attacks in June 2025. Threat actors primarily targeted government databases, but also impacted various sectors, including financial services, telecommunications, education, insurance, healthcare, the military, and even the sports industry.
- Access Breaches made up around 24% of the attacks and focused entirely on government systems across multiple countries.
- Ransomware was very rare this month, seen only once when the Nightspire group hit a government agency in South Africa.
- Vulnerabilities were also rare, with only one known case where an attacker exploited a weakness in an education system in Morocco and advertised the exploitation on the dark web.

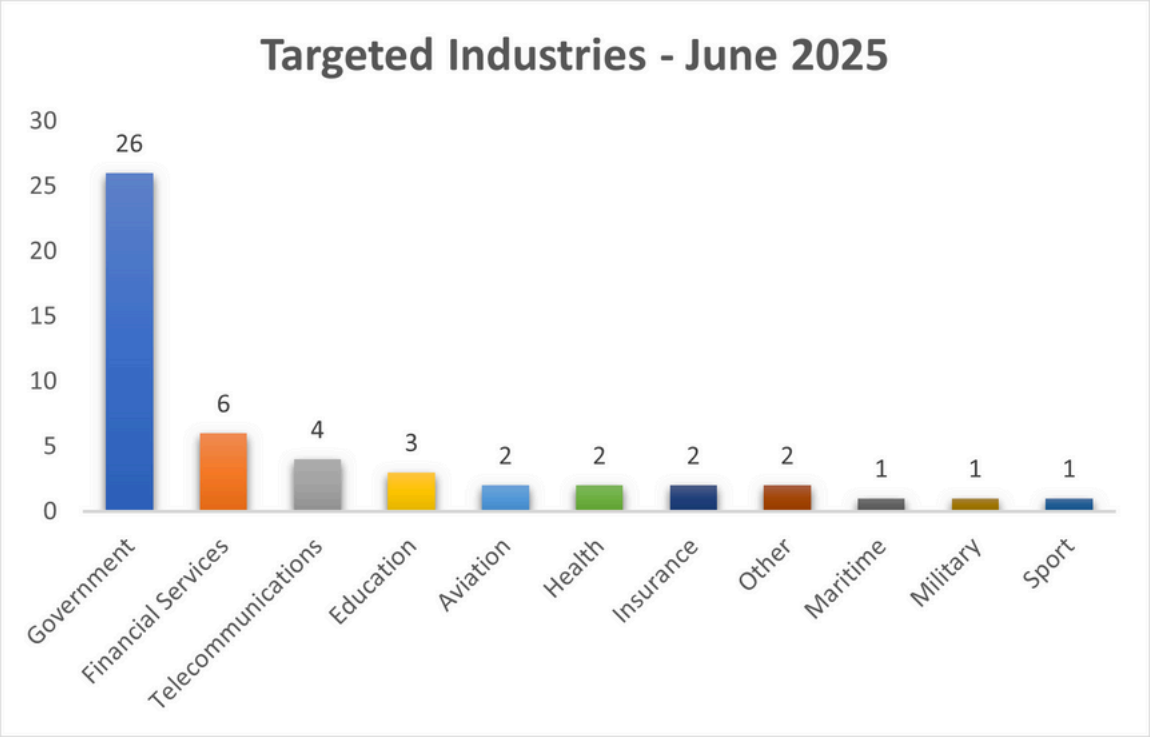
TOP RANSOMWARE GROUPS



Ransomware was not a major threat in Africa in June 2025. Only one group, Nightspire, was observed deploying ransomware.

- Nightspire targeted a government agency in South Africa, making it the only recorded ransomware case for the month.

INDUSTRIES MOST TARGETED



The government sector was the most targeted in June 2025, with 26 incidents, continuing its trend as the primary focus for cyberattacks in Africa. This shows how vulnerable public systems remain in Africa.

Financial services followed closely, with banks and insurance platforms repeatedly targeted for their valuable data.

We also saw incidents across telecommunications, education, health, aviation, military, insurance, sport, and maritime sectors, proving that attackers will exploit any weakness, regardless of the industry.

THREAT LANDSCAPE IN MOROCCO & ALGERIA

In June 2025, cyber warfare between Morocco and Algeria intensified, with both countries experiencing politically motivated cyberattacks. Morocco faced a major breach of its National Social Security Fund (CNSS.ma), attributed to Algerian-linked actors, which triggered retaliatory attacks from a Moroccan hacktivist group called Phantom Atlas. This group targeted key Algerian institutions, including Algerie Telecom, MGPTT, and the Ministry of Labor, stealing and leaking sensitive data.

Simultaneously, Morocco dealt with internal attacks from groups like b4bayega, XrOOT01, and TajineSec, affecting sectors like government, finance, healthcare, and education.

On the Algerian side, a pro-Moroccan group named Server Dump launched attacks against several Algerian ministries, and even breached Tunisia's Ministry of Defense, signaling regional escalation.

These cyber operations reflect a growing trend of nationalist hacktivism and geopolitical retaliation in North Africa, with both civilian and government systems increasingly caught in the crossfire.

CONCLUSION

June 2025 highlighted just how much Africa's cyber threat landscape has evolved, and how vulnerable it remains. A handful of highly active threat actors were responsible for most attacks, exploiting weak database security and poor access controls to compromise sensitive systems. Their operations crossed borders and industries, showing that attackers' focus transcends any one type of data or sector.

Morocco and Algeria were the main hotspots this month. Their long-standing geopolitical tensions have now firmly spilt into cyberspace, fueling a wave of nationalist hacktivist campaigns. Groups like Server Dump and Phantom Atlas leveraged this climate to target Algeria's most critical institutions, including defense and customs, while Moroccan entities faced retaliatory attacks tied to Algerian sympathizers. This blend of politically motivated campaigns with traditional cybercrime makes the regional threat environment even more unpredictable.

Beyond regional politics, the data tells a broader story. Governments remain the primary targets, reflecting the immense value of state-held data and the often outdated defenses protecting it. But financial services, education, healthcare, insurance, military, telecommunications, aviation, maritime, and even sports were all impacted in June. This clearly signals that attackers are opportunistic. They will exploit any weakness, regardless of the industry, if it leads to valuable data or access.

The limited ransomware and sophisticated vulnerability exploits this month offer false relief. It only implies that attackers continue to favor the easiest and most scalable methods first: misconfigured databases and weak credentials. The risk of a shift back to more disruptive tactics, like widespread ransomware or supply chain attacks, remains ever-present.

Ultimately, these trends make one thing clear: Africa's cybersecurity strategies must evolve just as quickly as the threats. Countries need to invest heavily in securing their data at rest and in transit, enforcing strong identity and access controls, regularly patching systems, and building resilient incident response capabilities. Just as importantly, there must be increased collaboration across borders to address shared risks. Without a coordinated regional approach, individual defenses will continue to fall short against attackers who see no national boundaries.

RECOMMENDATIONS

To effectively respond to the threats observed in June 2025, here are some practical steps organizations across Africa should take:

- Encrypt all sensitive data, both at rest and in transit.
- Regularly audit databases for misconfigurations and eliminate unnecessary public access.
- Apply strict access controls and ensure users only have permissions essential to their roles.
- Enforce multi-factor authentication (MFA) across all critical systems, with special attention to administrator accounts.
- Monitor login patterns for suspicious activity, like unusual locations or failed login bursts, and set up alerts.
- Adopt strong password policies and require regular password changes to reduce credential theft risks.
- Maintain a rigorous patching cycle, especially for public-facing applications and legacy systems that attackers frequently exploit.
- Use security tools to continuously scan for vulnerabilities and address them without delay.
- Deploy detection systems that can spot abnormal behaviors such as unexpected large data transfers or odd working-hour logins.
- Develop and routinely test incident response plans so teams know exactly how to react when breaches occur.
- Conduct ongoing cybersecurity training so employees can recognize phishing and social engineering attempts, since many attacks start there.
- Extend security awareness efforts to contractors and third parties who may have access to your systems.
- Keep secure, offline backups of critical data and test restoration processes to prepare for ransomware scenarios.

RECOMMENDATIONS (CONT'D)

- Have a communication and legal plan ready in case of ransomware or extortion demands.
- Given the cross-border nature of threats, especially highlighted by activity in Morocco and Algeria, build cooperative relationships with neighboring countries to share intelligence and coordinate defenses.
- Participate in regional or sector-specific threat intelligence networks to gain early insights into campaigns that could affect your organization.

ABOUT US

CyHawk is Africa's open-source cyber threat intelligence platform dedicated to tracking, documenting, and exposing digital threats targeting individuals, organizations, and key sectors across the continent.

We analyze real-time threat data—from ransomware and data breaches to defacement and dark web activity, focusing exclusively on incidents affecting Africa. Our mission is to bridge the intelligence gap by providing publicly accessible, evidence-based reports that empower defenders, raise awareness, and support policy efforts across the continent.

What We Offer

- Monthly threat reports highlighting emerging actors and trends
- Dark web monitoring for African-related leaks, sales, and chatter
- Blog posts & incident analyses breaking down complex attacks
- Awareness campaigns focused on education and resilience

We believe cybersecurity in Africa must be community-driven, transparent, and locally relevant.

Learn More

Visit us at www.cyhawk-africa.com
For collaborations, tips, or threat submissions:
info@cyhawk-africa.com